EMPFEHLUNGEN

EMPFEHLUNG (EU) 2019/534 DER KOMMISSION

vom 26. März 2019

Cybersicherheit der 5G-Netze

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 292,

in Erwägung nachstehender Gründe:

(1) Die Kommission sieht die Einführung von Netztechnik der 5. Generation (5G) als wichtige Voraussetzung für künftige digitale Dienste und als eine Priorität der Strategie für einen digitalen Binnenmarkt. Sie hat den 5G-Aktionsplan angenommen, um sicherzustellen, dass die Union ab 2020 über die für ihren digitalen Wandel erforderlichen Vernetzungsinfrastrukturen verfügt ([1]).

(2) Die 5G-Netze werden auf der derzeitigen Netztechnik der 4. Generation (4G) aufbauen; sie werden neue Dienstekapazitäten bereitstellen und zur zentralen Infrastruktur und Triebkraft für weite Teile der Wirtschaft der Union werden. Sobald die 5G-Netze eingeführt sind, werden sie das Rückgrat eines breiten Spektrums von Diensten bilden, die für das Funktionieren des Binnenmarkts, die Aufrechterhaltung und Ausführung wichtiger gesellschaftlicher und wirtschaftlicher Funktionen — wie Energie, Verkehr, Bank- und Gesundheitswesen — sowie industrieller Steuerungssysteme unverzichtbar sind. Die Organisation demokratischer Prozesse, z. B. von Wahlen, wird sich mehr und mehr auf digitale Infrastrukturen und 5G-Netze stützen.

(3) Aufgrund der Abhängigkeit vieler kritischer Dienste von 5G-Netzen wären die Folgen systemischer und weitverbreiteter Störungen besonders gravierend. Daher ist die Gewährleistung der Cybersicherheit von 5G-Netzen ein Thema von strategischer Bedeutung für die Union in einer Zeit, in der Cyberangriffe zunehmen und immer komplexer werden.

(4) Aufgrund der Vernetzung und des transnationalen Charakters der Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen, sowie des grenzübergreifenden Charakters der betreffenden Bedrohungen würden sich alle erheblichen Schwachstellen und/oder Cybersicherheitsvorfälle, die 5G-Netze in einem Mitgliedstaat betreffen, auf die Union als Ganzes auswirken. Deshalb sollten Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus der 5G-Netze getroffen werden.

(5) Die Mitgliedstaaten haben bestätigt, dass Handlungsbedarf auf Unionsebene besteht. Laut seinen Schlussfolgerungen vom 21. März 2019 sieht der Europäische Rat der Empfehlung der Kommission zu einem abgestimmten Vorgehen bei der Sicherheit von 5G-Netzen erwartungsvoll entgegen ([2]).

(6) Die Wahrung der europäischen Souveränität unter uneingeschränkter Achtung der europäischen Werte der Offenheit und Toleranz sollte ein wichtiges Ziel sein ([3]). Ausländische Investitionen in strategischen Sektoren, der Erwerb kritischer Anlagen, Technologien und Infrastrukturen in der Union sowie die Versorgung mit kritischen Ausrüstungen können ebenfalls eine Gefahr für die Sicherheit der Union darstellen.

(7) Die Cybersicherheit der 5G-Netze ist von entscheidender Bedeutung für die Gewährleistung der strategischen Autonomie der Union, wie in der Gemeinsamen Mitteilung „EU-China — Strategische Perspektiven“ ([4]) anerkannt wird.

(8) In der Entschließung des Europäischen Parlaments zu Sicherheitsbedrohungen im Zusammenhang mit der zunehmenden technologischen Präsenz Chinas in der EU ([5]) werden die Kommission und die Mitgliedstaaten ebenfalls aufgefordert, Maßnahmen auf Unionsebene zu ergreifen.

(9) In dieser Empfehlung werden Leitlinien für geeignete Risikoanalyse- und -managementmaßnahmen auf nationaler Ebene, für die Entwicklung einer koordinierten europäischen Risikobewertung und für die Einrichtung eines Verfahrens zur Entwicklung eines gemeinsamen Instrumentariums bewährter Risikomanagementmaßnahmen dargelegt, die der Bekämpfung von Cybersicherheitsrisiken in 5G-Netzen dienen sollen.

(10) Es gibt einen starken Rechtsrahmen für den Schutz elektronischer Kommunikationsnetze in der Union.

([1]) COM(2016) 588 final.
([2]) Schlussfolgerungen des Europäischen Rates vom 21. und 22. März 2019.
([3]) Rede zur Lage der Union 2018 — Die Stunde der europäischen Souveränität, 12. September 2018.
([4]) JOIN(2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//DE.

(11) Der Rechtsrahmen der Union im Bereich der elektronischen Kommunikation ([6]) fördert den Wettbewerb, den Binnenmarkt und die Interessen der Endnutzer und verfolgt in Verbindung mit dem Europäischen Kodex für die elektronische Kommunikation ([7]) ein zusätzliches Konnektivitätsziel in Form der folgenden Ergebnisse: flächendeckende Einführung und Nutzung von Netzen mit sehr hoher Kapazität für alle Bürger und Unternehmen der Union unter Wahrung der Interessen der Bürgerinnen und Bürger. Gemäß der Richtlinie 2002/21/EG müssen die Mitgliedstaaten dafür sorgen, dass die Integrität und Sicherheit der öffentlichen Kommunikationsnetze gewährleistet wird und dass Unternehmen, die öffentliche Kommunikationsnetze bereitstellen oder öffentlich zugängliche elektronische Kommunikationsdienste erbringen, verpflichtet sind, hinreichende technische und organisatorische Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten zu ergreifen. In der Richtlinie ist ferner vorgesehen, dass die zuständigen nationalen Regulierungsbehörden u. a. befugt sind, verbindliche Anweisungen zu erteilen, um die Einhaltung dieser Verpflichtungen sicherzustellen.

(12) Darüber hinaus gestattet die Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates ([8]) den Mitgliedstaaten, Bedingungen im Hinblick auf den Schutz öffentlicher Netze gegen unbefugten Zugang an die Allgemeingenehmigung zu knüpfen, um die Vertraulichkeit der Kommunikation gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([9]) zu wahren.

(13) Um die Umsetzung dieser Verpflichtungen zu unterstützen, hat die Union eine Reihe von Kooperationsgremien eingerichtet. Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), die Kommission, die Mitgliedstaaten und die nationalen Regulierungsbehörden haben technische Leitlinien für die nationalen Regulierungsbehörden in Bezug auf die Meldung von Sicherheitsvorfällen, Sicherheitsmaßnahmen und Bedrohungen und Vermögenswerte ([10]) ausgearbeitet. In der mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([11]) eingesetzten Kooperationsgruppe (im Folgenden die „Kooperationsgruppe“) kommen die zuständigen Behörden zusammen, um die Zusammenarbeit zu unterstützen und zu erleichtern, indem sie insbesondere strategische Vorgaben für die Tätigkeiten des Netzes der Computer-Notfallteams (*Computer Security Incident Response Teams*) machen, um die operative Zusammenarbeit auf technischer Ebene zu vereinfachen.

(14) Der künftige europäische Rahmen für die Cybersicherheitszertifizierung ([12]) sollte ein wesentliches unterstützendes Instrument bilden, um ein kohärentes Sicherheitsniveau zu fördern. Dies sollte die Entwicklung von Systemen für die Cybersicherheitszertifizierung ermöglichen, die den Bedürfnissen der Nutzer von 5G-Geräten und -Software entsprechen. Aufgrund der wesentlichen Bedeutung dieser Infrastrukturen sollte die Entwicklung einschlägiger europäischer Systeme für die Cybersicherheitszertifizierung von Produkten, Dienstleistungen oder Prozessen der Informations- und Kommunikationstechnik, die für 5G-Netze genutzt werden, eine unmittelbare Priorität darstellen. Die Mitgliedstaaten und die Marktteilnehmer sollten sich aktiv an der Entwicklung solcher Zertifizierungssysteme beteiligen und u. a. die Festlegung spezifischer Schutzprofile für 5G-Netze unterstützen.

(15) In Ermangelung harmonisierter Unionsrechtsvorschriften können die Mitgliedstaaten im Wege von nationalen technischen Vorschriften, die im Einklang mit dem Unionsrecht verabschiedet worden sind, festlegen, dass ein europäisches System für die Cybersicherheitszertifizierung Pflicht sein sollte. Die Mitgliedstaaten können auch im Rahmen der öffentlichen Auftragsvergabe und der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates ([13]) auf europäische Systeme für die Cybersicherheitszertifizierung zurückgreifen und könnten die Entwicklung von Hilfsmechanismen wie z. B. einer Beratungsplattform für den Erwerb von Cybersicherheitslösungen durch öffentliche Auftraggeber unterstützen.

(16) Ein hohes Maß an Datenschutz und Privatsphäre ist ein wichtiger Faktor, um die Sicherheit der 5G-Netze zu gewährleisten. Auch auf Unionsebene wurden Vorschriften festgelegt, die die Sicherheit der Verarbeitung personenbezogener Daten u. a. im Bereich der elektronischen Kommunikation gewährleisten. In der Datenschutz-Grundverordnung ([14]) ist die Verpflichtung verankert, dass personenbezogene Daten so verarbeitet werden sollen,

---

([6]) Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie) (ABl. L 108 vom 24.4.2002, S. 33) und die spezifischen Richtlinien.

([7]) Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).

([8]) Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie) (ABl. L 108 vom 24.4.2002, S. 21).

([9]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

([12]) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)(COM(2017) 477 final — 2017/0225 (COD)).

([13]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EGABl. L 94 vom28.3.2014, S. 65).

([14]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

dass ihre Sicherheit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben/erhalten und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können. Die Datenschutzrichtlinie für elektronische Kommunikation enthält besondere Vorschriften über den Schutz der Vertraulichkeit der Kommunikation und der Endgeräte der Nutzer. Außerdem werden Diensteanbieter dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Sicherheit ihrer Dienste zu gewährleisten.

(17) Die Union hat außerdem ein Rechtsinstrument verabschiedet, mit dem kritische Infrastrukturen und Technologien wie jene, die in der Kommunikation genutzt werden, geschützt werden können, indem den Mitgliedstaaten gestattet wird' ausländische Direktinvestitionen aus Gründen der Sicherheit und der öffentlichen Ordnung zu überprüfen, und indem ein Kooperationsmechanismus geschaffen wird, der es den Mitgliedstaaten und der Kommission ermöglicht, Informationen auszutauschen und Bedenken in Bezug auf bestimmte Investitionen zu äußern ([15]).

(18) Die Mitgliedstaaten und die Betreiber treffen derzeit wichtige vorbereitende Schritte, um die groß angelegte Einführung von 5G-Netzen zu ermöglichen. Mehrere Mitgliedstaaten haben im Zusammenhang mit der Durchführung der Verfahren zur Erteilung von Nutzungsrechten für Funkfrequenzen, die für 5G-Netze bestimmt sind ([16]), Bedenken hinsichtlich potenzieller Sicherheitsrisiken der 5G-Netze geäußert und Maßnahmen zur Bewältigung dieser Risiken geprüft.

(19) Bei der Bewältigung von Cybersicherheitsrisiken in 5G-Netzen sollten sowohl technische als auch andere Faktoren berücksichtigt werden. Zu den technischen Faktoren können Schwachstellen im Bereich der Cybersicherheit zählen, die für den unberechtigten Zugriff auf Informationen (z. B. Cyberspionage aus wirtschaftlichen oder politischen Gründen) oder für andere böswillige Zwecke (Cyberangriffe zur Störung oder Zerstörung von Systemen und Daten) genutzt werden können. Zu prüfen wäre, ob die Netze über ihren gesamten Lebenszyklus hinweg geschützt werden müssen und ob alle einschlägigen Ausrüstungen auch in den Entwurfs-, Entwicklung-, Auftragsvergabe, Einführungs-, Betriebs- und Wartungsphasen der 5G-Netze in diesen Schutz einbezogen werden müssen.

(20) Weitere Faktoren können regulatorische oder sonstige Anforderungen an die Anbieter von Informations- und Kommunikationstechnik betreffen. Bei einer Bewertung der Bedeutung solcher Faktoren wäre unter anderem dem allgemeinen Risiko eines Einflusses eines Drittlands, insbesondere in Bezug auf das Governance-Modell, dem Fehlen von Kooperationsvereinbarungen über die Sicherheit oder ähnlicher Regelungen wie Angemessenheitsbeschlüsse in Bezug auf den Datenschutz zwischen der Union und dem betreffenden Drittland oder der Frage, ob dieses Land Vertragspartei multilateraler, internationaler oder bilateraler Abkommen über Cybersicherheit, die Bekämpfung der Cyberkriminalität oder den Datenschutz ist, Rechnung zu tragen.

(21) Als wichtiger Schritt zur Entwicklung eines Unionskonzepts für die Cybersicherheit von 5G-Netzen sollte eine Risikobewertung auf nationaler Ebene durchgeführt und abgeschlossen werden. Dies würde den Mitgliedstaaten dabei helfen, die nationalen Maßnahmen in Bezug auf die Sicherheitsanforderungen und das Risikomanagement im Lichte dieser Bewertung anzupassen.

(22) Es sollten Koordinierungsmaßnahmen entwickelt werden, um die Wirksamkeit von Maßnahmen zur Bewältigung dieser Cybersicherheitsbedrohungen zu gewährleisten, die für das reibungslose Funktionieren des Binnenmarkts und den Schutz personenbezogener Daten und der Privatsphäre von wesentlicher Bedeutung sind.

(23) Die nationalen Risikobewertungen sollten die Grundlage für eine koordinierte Risikobewertung auf Unionsebene bilden, die sich aus einer Erfassung der Bedrohungslage und einer gemeinsamen Überprüfung durch die Mitgliedstaaten mit Unterstützung der Kommission und in Zusammenarbeit mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) zusammensetzt.

(24) Unter Berücksichtigung der Risikobewertungen auf Ebene der Mitgliedstaaten und der Union sollte die Kooperationsgruppe eine Instrumentarium schaffen, mit dem Arten von Cybersicherheitsrisiken und möglichen Maßnahmen zur Minderung der Risiken in Bereichen wie Zertifizierung, Erprobung und Zugangskontrollen ermittelt werden können. Sie sollte ferner mögliche spezifische Maßnahmen bestimmen, die geeignet sind, gegen die von einem oder mehreren Mitgliedstaaten ermittelten Risiken vorzugehen. Die Kooperationsgruppe sollte die Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA), von Europol, des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) und des EU-Zentrums für Informationsgewinnung und -analyse in Anspruch nehmen. Dieses Instrumentarium sollte dazu dienen, die Kommission bei der Ausarbeitung gemeinsamer Mindestanforderungen für die weitere Gewährleistung eines hohen Cybersicherheitsniveaus von 5G-Netzen in der gesamten Union zu unterstützen.

(25) Wenn Maßnahmen zur Bewältigung der Cybersicherheitsrisiken ergriffen werden, sollte beim Aufbau eines einheitlichen Netzes bedacht werden, die Cybersicherheit durch Anbietervielfalt zu fördern.

([15]) Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union (ABl L 79I vom 21.3.2019, S. 1.).

([16]) Das Auktionsverfahren für mindestens ein Frequenzband ist in elf Mitgliedstaaten (Belgien, Tschechien, Deutschland, Irland, Griechenland, Frankreich, Litauen, Ungarn, Niederlande, Österreich, Portugal) für 2019 vorgesehen. Für 2020 sind sechs weitere Auktionen geplant (in Spanien, Litauen (andere Frequenzen), Malta, Polen, Slowakei, Vereinigtes Königreich). Quelle: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich, einschließlich des Rechts der Mitgliedstaaten, Anbieter oder Lieferanten aus Gründen der nationalen Sicherheit von ihren Märkten auszuschließen, bleiben von dieser Empfehlung unberührt —

HAT FOLGENDE EMPFEHLUNG ABGEGEBEN:

I. **ZIELE**

(1) Um die Entwicklung eines Unionskonzepts zur Gewährleistung der Cybersicherheit von 5G-Netzen zu unterstützen, werden in dieser Empfehlung Maßnahmen bestimmt, die ergriffen werden sollten, um Folgendes zu erreichen:

a) Bewertung der Cybersicherheitsrisiken, die 5G-Netze auf nationaler Ebene betreffen, und Ergreifung der erforderlichen Sicherheitsmaßnahmen durch die Mitgliedstaaten;

b) gemeinsame Entwicklung einer koordinierten Risikobewertung auf Unionsebene, die auf der nationalen Risikobewertung aufbaut, durch die Mitgliedstaaten und die einschlägigen Organen, Agenturen und sonstigen Einrichtungen der Union;

c) Bestimmung möglicher gemeinsamer Maßnahmen, die zur Minderung der Cybersicherheitsrisiken im Zusammenhang mit Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen, insbesondere 5G-Netzen, ergriffen werden können, durch die mit der Richtlinie (EU) 2016/1148 eingesetzte Kooperationsgruppe.

II. **BEGRIFFSBESTIMMUNGEN**

(2) Für die Zwecke dieser Empfehlung gelten folgende Begriffsbestimmungen:

a) „5G-Netze“ bezeichnet eine Gesamtheit einschlägiger Netzinfrastrukturelemente, die auf weltweit vereinbarten technischen Normen für die Mobilfunk- und Drahtloskommunikation beruhen, für Netzanbindungs- und Mehrwertdienste verwendet werden und fortgeschrittene Leistungsmerkmale wie sehr hohe Datengeschwindigkeit und -kapazität, Kommunikation mit niedriger Latenzzeit, ultra-hohe Zuverlässigkeit oder Unterstützung einer großen Zahl verbundener Geräte aufweisen. Dies kann auch vorhandene Netzbestandteile umfassen, denen frühere Generationen mobiler und drahtloser Kommunikationstechnik (4G oder 3G) zugrunde liegen. 5G-Netze sind so zu verstehen, dass sie alle einschlägigen Teile des Netzes umfassen;

b) „Infrastrukturen, die dem digitalen Ökosystem zugrunde liegen“ bezeichnet Infrastrukturen, die der Digitalisierung über ein breites Spektrum kritischer Anwendungen in Wirtschaft und Gesellschaft hinweg dienen.

III. **MASSNAHMEN AUF NATIONALER EBENE**

(3) Die Mitgliedstaaten sollten bis zum 30. Juni 2019 eine Risikobewertung der 5G-Netzinfrastruktur durchführen, einschließlich der Bestimmung der sensibelsten Elemente, bei denen Sicherheitsvorfälle erhebliche negative Auswirkungen nach sich ziehen würden. Bis zum selben Zeitpunkt sollten die Mitgliedstaaten auch die auf nationaler Ebene geltenden Sicherheitsanforderungen und Risikomanagementverfahren überprüfen, sodass sie Bedrohungen der Cybersicherheit Rechnung tragen, die sich aus i) technischen Faktoren, wie den spezifischen technischen Merkmalen der 5G-Netze, und ii) anderen Faktoren wie den rechtlichen und politischen Rahmenbedingungen, denen Anbieter von Informations- und Kommunikationstechnik in Drittländern unterliegen können, ergeben können.

(4) Auf der Grundlage dieser nationalen Risikobewertung und Überprüfung und unter Berücksichtigung der laufenden koordinierten Maßnahmen auf Unionsebene sollten die Mitgliedstaaten

a) die für 5G-Netze geltenden Sicherheitsanforderungen und die entsprechend angewandten Risikomanagementverfahren aktualisieren;

b) die einschlägigen Verpflichtungen für Unternehmen, die öffentliche Kommunikationsnetze bereitstellen oder öffentlich zugängliche elektronische Kommunikationsdienste erbringen, gemäß den Artikeln 13a und 13b der Richtlinie 2002/21/EG aktualisieren;

c) Bedingungen im Hinblick auf den Schutz öffentlicher Netze gegen unbefugten Zugang an die Allgemeingenehmigung knüpfen und die Unternehmen, die an künftigen Verfahren zur Erteilung von Nutzungsrechten für Funkfrequenzen in 5G-Frequenzbändern gemäß der Richtlinie 2002/20/EG teilnehmen, zur Einhaltung der Sicherheitsanforderungen für Netze verpflichten;

d) weitere Präventivmaßnahmen zur Minderung potenzieller Cybersicherheitsrisiken anwenden.

(5) Im Rahmen der in Nummer 4 genannten Maßnahmen sollten gegebenenfalls die Anbieter und Betreiber verpflichten werden, für die Sicherheit der sensiblen Teile der Netze zu sorgen und gegebenenfalls den zuständigen nationalen Behörden einschlägige Informationen über geplante Änderungen der elektronischen Kommunikationsnetze zur Verfügung zu stellen und spezifische Komponenten und Systeme der Informationstechnik im Hinblick auf Sicherheit und Integrität vorab von nationalen Prüfstellen/Zertifizierungslaboratorien testen zu lassen.

(6) Gemeinsame Sicherheitsüberprüfungen sollten von zwei oder mehr Mitgliedstaaten durchgeführt werden, wobei die geeigneten technischen Fachkenntnisse und Einrichtungen im Zusammenhang mit Infrastrukturen, die dem digitalen Ökosystem und den 5G-Netzen zugrunde liegen, zu nutzen und weiterzugeben sind, beispielsweise wenn dasselbe Unternehmen in mehr als einem Mitgliedstaat eine Netzinfrastruktur betreibt oder aufbaut oder wenn große Ähnlichkeiten in den Netzkonfigurationen bestehen. Die Agentur der Europäischen Union für Cybersicherheit (ENISA), Europol und das Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) sollten Unterstützungsersuchen der Mitgliedstaaten in diesem Bereich Vorrang einräumen. Die Ergebnisse dieser Überprüfungen sollten der Kooperationsgruppe und dem Netz der Computer-Notfallteams (CSIRT) übermittelt werden.

IV. KOORDINIERTES VORGEHEN AUF UNIONSEBENE

(7) Um ein gemeinsames Konzept zur Bewältigung der Cybersicherheitsrisiken in Bezug auf 5G-Netze zu entwickeln, sollten die Mitgliedstaaten bis zum 30. April 2019 diesbezügliche Arbeiten in einem eigenen Bereich der Kooperationsgruppe aufnehmen. Die Mitgliedstaaten sollten die zuständigen Behörden auffordern, sich gegebenenfalls an der Arbeit der Kooperationsgruppe zu beteiligen.

Eine koordinierte europäische Risikobewertung

(8) Die Mitgliedstaaten sollten untereinander und mit den einschlägigen Einrichtungen der Union Informationen austauschen, um ein gemeinsames Bewusstsein für die bestehenden und die potenziellen Cybersicherheitsrisiken zu schaffen, die mit 5G-Netzen verbunden sind.

(9) Die Mitgliedstaaten sollten der Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) bis zum 15. Juli 2019 ihre nationalen Risikobewertungen übermitteln.

(10) Die Agentur der Europäischen Union für Cybersicherheit (ENISA) sollte die spezifische Bedrohungslage der 5G-Netze erfassen. Die Kooperationsgruppe und das Netz der Computer-Notfallteams, die mit der Richtlinie (EU) 2016/1148 eingerichtet wurden, sollten diesen Vorgang unterstützen.

(11) Unter Berücksichtigung all dieser Elemente sollten die Mitgliedstaaten mit Unterstützung der Kommission und gemeinsam mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) bis zum 1. Oktober 2019 eine gemeinsame Überprüfung der unionsweiten Exposition gegenüber Risiken im Zusammenhang mit Infrastrukturen, die dem digitalen Ökosystem, insbesondere 5G-Netzen, zugrunde liegen, durchführen.

(12) Bei dieser gemeinsamen Überprüfung sollten vorrangig die Risiken analysiert werden, die die besonders sensiblen oder gefährdeten Elemente des Betriebs und der Wartung, einschließlich der Kernbestandteile der 5G-Netze, sowie die 5G-Netzzugriffselemente für industrielle Anwendungen betreffen.

(13) In einer zweiten Phase sollte diese gemeinsame Überprüfung auf weitere strategische Elemente der digitalen Wertschöpfungskette ausgedehnt werden.

Ein gemeinsames Unionsinstrumentarium zur Bewältigung der Risiken

(14) Im Rahmen der Arbeit der Kooperationsgruppe sollten bewährte Verfahren und Maßnahmen der in Nummer 4 genannten Art ermittelt werden, die auf nationaler Ebene angewandt werden. Auf der Grundlage dieser nationalen bewährten Verfahren sollte bis zum 31. Dezember 2019 ein Instrumentarium mit geeigneten, wirksamen und angemessenen möglichen Risikomanagementmaßnahmen zur Minderung der auf nationaler und Unionsebene ermittelten Cybersicherheitsrisiken vereinbart werden, um die Kommission bei der Ausarbeitung gemeinsamer Mindestanforderungen für die weitere Gewährleistung eines hohen Cybersicherheitsniveaus von 5G-Netzen in der gesamten Union zu unterstützen.

(15) Dieses Instrumentarium sollte Folgendes umfassen:

a) eine Bestandsaufnahme der Arten von Sicherheitsrisiken, die die Cybersicherheit von 5G-Netzen beeinträchtigen können (z. B. Risiko für die Lieferkette, Risiko durch Softwareschwachstellen, Risiko in Bezug auf die Zugangskontrollen, Risiken, die sich aus den rechtlichen und politischen Rahmenbedingungen, denen Anbieter von Informations- und Kommunikationstechnik in Drittländern unterliegen können, ergeben), und

b) eine Reihe möglicher Risikominderungsmaßnahmen (z. B. Hardware-, Software- oder Dienstezertifizierung durch Dritte, formelle Erprobung von Hardware und Software oder Konformitätskontrollen, Verfahren zur Gewährleistung der Zugangskontrollen und ihrer Durchsetzung, Bestimmung von Produkten, Diensten oder Anbietern, die möglicherweise als nicht sicher anzusehen sind usw.). Diese Maßnahmen sollten alle Arten von Sicherheitsrisiken berücksichtigen, die im Rahmen der Risikobewertungen in einem oder mehreren Mitgliedstaaten ermittelt wurden.

(16) Sobald die europäischen Systeme für die Cybersicherheitszertifizierung für 5G-Netze zur Verfügung stehen, sollten die Mitgliedstaaten im Einklang mit dem Unionsrecht nationale technische Vorschriften erlassen, die die verbindliche Zertifizierung von Produkten, Diensten oder Systemen der Informations- und Kommunikationstechnik, die unter diese Systeme fallen, vorsehen.

(17) Die Mitgliedstaaten sollten gemeinsam mit der Kommission an die Allgemeingenehmigung zu knüpfende Bedingungen im Hinblick auf den Schutz öffentlicher Netze gegen unbefugten Zugang sowie Sicherheitsanforderungen für Netze bestimmen, die Unternehmen, die an künftigen Verfahren zur Erteilung von Nutzungsrechten für Funkfrequenzen in 5G-Frequenzbändern gemäß der Richtlinie 2002/20/EG teilnehmen, auferlegt werden. Diese Verpflichtungen sollten, soweit möglich, in den Maßnahmen nach Absatz 4 Buchstabe c berücksichtigt werden.

(18) Die Mitgliedstaaten sollten mit der Kommission zusammenarbeiten, um spezifische Sicherheitsanforderungen auszuarbeiten, die im Zusammenhang mit der Vergabe öffentlicher Aufträge in Bezug auf 5G-Netze gelten könnten. Dies sollte verbindliche Anforderungen zur Umsetzung von Systemen für die Cybersicherheitszertifizierung bei der Vergabe öffentlicher Aufträge umfassen, sofern solche Systeme nicht bereits für alle Anbieter und Betreiber verbindlich sind.

V. **ÜBERPRÜFUNG**

(19) Die Mitgliedstaaten sollten mit der Kommission zusammenarbeiten, um die Auswirkungen dieser Empfehlung im Hinblick auf die Festlegung geeigneter Vorgehensweisen bis zum 1. Oktober 2020 zu bewerten. Bei dieser Bewertung sollten die Ergebnisse der koordinierten Risikobewertung der Union und das Unionsinstrumentarium berücksichtigt werden.

Straßburg, den 26. März 2019

Für die Kommission

Julian KING

Mitglied der Kommission